

IN THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application.

1 1. (Currently amended) A method of examining a network, including:
2 identifying an operating system of a remote host based on communications with
3 the remote host through the network, including identifying a version and a
4 patch level of the operating system;
5 identifying a service of the remote host based on the communications, ~~with the~~
6 ~~remote host through the network~~, including identifying a version and a
7 patch level of the service; and
8 identifying a vulnerability of the network based on at least one of the identified
9 operating system and the identified service, ~~information obtained from the~~
10 ~~steps of identifying an operating system and identifying a service.~~

1 2. (Currently amended) The method of claim 1, wherein:
2 ~~the step of~~ identifying an operating system includes sending a first set of packets
3 to the remote host and receiving a second set of packets from the remote
4 host in response to the ~~said~~ first set of packets, and analyzing the second
5 set of packets for inferential information indicative of the operating
6 system; and
7 ~~the step of~~ identifying a service includes sending a third set of packets to the
8 remote host and receiving a fourth set of packets from the remote host in
9 response to the ~~said~~ third set of packets, wherein information contained in
10 the ~~said~~ third set of packets is based on information received in the ~~said~~
11 second set of packets, and analyzing the fourth set of packets for
12 inferential information indicative of the service; ~~and~~
13 ~~the step of identifying a vulnerability includes comparing information contained~~
14 ~~in the second set of packets and the fourth set of packets to preexisting~~
15 ~~vulnerability information in a database.~~

1 3. (Currently amended) The method of claim 1, wherein ~~the step of~~
2 identifying an operating system includes sending three sets of packets to the remote host
3 and receiving three respective sets of responsive packets from the remote host.

1 4. (Currently amended) A method of examining a network, including:
2 nonintrusively identifying an operating system of a remote host including
3 identifying a version of the operating system based on inferential
4 information received from the remote host in headers of packets; and
5 nonintrusively identifying a service of the remote host including identifying a
6 version of the service based on the inferential information, ~~received from~~
7 ~~the remote host.~~

1 5. (Currently amended) The method of claim 4, further including:
2 identifying a vulnerability of the network based on at least one of the identified
3 operating system and the identified service.

1 6. (Currently amended) The method of claim 4, further including:
2 identifying the identified service as a trojan application on the remote host.

1 7. (Currently amended) The method of claim 4, further including:
2 identifying the identified service as an unauthorized software use on the remote
3 host.

1 8. (Currently amended) The method of claim 4, further including:
2 identifying a security policy violation ~~violations~~ on the network based on the
3 inferential information.

1 9. (Currently amended) The method of claim 4, wherein:
2 ~~the step of~~ identifying an operating system further includes identifying a patch
3 level of the operating system, ~~and~~

4 the step of identifying a service further includes identifying a patch level of the
5 service.

1 10. (Currently amended) The method of claim 4, wherein the steps of
2 identifying an operating system and identifying a service each includes:
3 sending a test selected packet to the remote host; and
4 receiving from the remote host a reflexive ~~responsive~~ packet containing at least a
5 portion of the inferential information.

1 11. (Canceled)

1 12. (Currently amended) The method of claim 4, wherein:
2 ~~the step of~~ identifying an operating system includes sending a first set of packets
3 to the remote host and receiving a second set of packets from the remote
4 host in response to the said first set of packets, the second set of packets
5 containing at least a portion of the inferential information; and
6 ~~the step of~~ identifying a service includes sending a third set of packets to the
7 remote host and receiving a fourth set of packets from the remote host in
8 response to the said third set of packets, the fourth set of packets
9 containing at least a portion of the inferential information.

1 13-18. (Canceled)

1 19. (Currently amended) A method of examining a network, including:
2 sending a set of test selected packets to a remote host on the network, at least part
3 of the first set of test packets including header information to generate a
4 response from the remote host that varies depending upon an operating
5 system and a service on the remote host;
6 receiving from the remote host a set of reflexive ~~responsive~~ packets responsive to
7 the test packets; and
8 identifying conditions of the remote host by using inferential information received
9 in the reflexive ~~responsive~~ packets, wherein the conditions include at least

10 one of the operating system and the service on the remote host, an-
11 operating system of the host, and a service of the host.

1 20. (Original) The method of claim 19, wherein the conditions further include
2 a vulnerability of the remote host.

1 21. (Original) The method of claim 19, wherein the conditions further include
2 the presence of unauthorized software on the remote host.

1 22. (Original) The method of claim 19, wherein the conditions include the
2 presence of a trojan application on the remote host.

1 23. (Previously presented) The method of claim 19, wherein:
2 identifying an operating system includes identifying a version; and
3 identifying a service includes identifying a version.

1 24. (Previously presented) The method of claim 19, wherein:
2 identifying an operating system includes identifying a version and a patch level;
3 and
4 identifying a service includes identifying a version and a patch level.

1 25. (Canceled)

1 26. (Currently amended) A method of detecting a vulnerability of a network,
2 comprising:
3 sending a first set of test packets to a remote host on the network;
4 receiving a first set of reflexive packets from the remote host in response to the
5 first set of test packets, at least part of the first set of reflexive packets
6 including header information that is unique to an operating system;
7 inferring the operating system;

8 sending a second set of test packets to the remote host; ~~on the network, wherein~~
9 ~~information contained in the first set of test packets is based on inferential~~
10 ~~information contained in the first set of reflexive packets;~~
11 receiving a second set of reflexive packets from the remote host in response to the
12 second set of test packets, at least part of the second set of reflexive
13 packets including header information that is unique to a service; and
14 inferring the service.
15 ~~based on inferential information contained in the first set of reflexive packets,~~
16 ~~identifying an operating system of the remote host, including a version and~~
17 ~~a patch level; and~~
18 ~~based on inferential information contained in the second set of reflexive packets,~~
19 ~~identifying a service of the remote host, including a version and a patch~~
20 ~~level.~~

1 27. (Canceled)

1 28. (Currently amended) The method of claim 26 27, further including:
2 ~~based on information contained in at least the tenth sequence, identifying a~~
3 vulnerability based on at least one of the inferred operating system and the
4 inferred service.

1 29. (Currently amended) The method of claim 26, wherein:
2 the first set of test packets includes:
3 a SYN Packet with false flag in the TCP option header;
4 a Fragmented UPD packet with malformed header (any header
5 inconsistency is sufficient), where the packet is 8K in size;
6 a FIN Packets of a selected variable size or a FIN packet without the ACK
7 or SYN flag properly set; and
8 a generic, well-formed ICMP ECHO request packet;
9 ~~the third set of packets includes:~~
10 a generic well-formed TCP Header set to 1024 bytes in size;
11 a Packet requesting an ICMP Timestamp;

12 a Packet with min/max segment size set to a selected variable value; and
13 a UDP packet with the fragment bit set;
14 ~~the fifth set of packets includes:~~
15 a TCP Packet with the header and options set incorrectly;
16 a well-formed ICMP Packet;
17 a Fragmented TCP or UDP packet;
18 a packet with an empty TCP window or a window set to zero;
19 a generic TCP Packet with 8K of random data; and
20 a SYN Packet with ACK and RST flags set.

1 30. (Previously presented) A method of examining a network, comprising:
2 sending a plurality of packets to a host on the network;
3 receiving a responsive plurality of packets from the host;
4 comparing inferential information in the responsive packets to information stored
5 in a database; and
6 based on the comparison, identifying a plurality of network conditions, including
7 a vulnerability of the network.

1 31. (Previously presented) A method of examining a network, comprising:
2 sending packets to a host on the network;
3 receiving responsive packets from the host;
4 comparing inferential information in the responsive packets to information stored
5 in a database; and
6 based on the comparison, identifying a trojan application on the network.

1 32. (Previously presented) A method of examining a network, comprising:
2 sending packets to a host on the network;
3 receiving responsive packets from the host;
4 comparing inferential information in the responsive packets to information stored
5 in a database; and
6 based on the comparison, identifying unauthorized software use on the network.

1 33. (Previously presented) A method of examining a network, comprising:
2 sending packets to a host on the network;
3 receiving responsive packets from the host;
4 comparing inferential information in the responsive packets to information stored
5 in a database; and
6 based on the comparison, inferring an unknown vulnerability.

1 34. (Previously presented) A method of examining a network, comprising:
2 sending packets to a host on the network;
3 receiving responsive packets from the host;
4 comparing inferential information in the responsive packets to information stored
5 in a database; and
6 based on the comparison, identifying a security policy violation.

1 35. (Canceled)

1 36. (Currently amended) A system for examining a network, comprising:
2 ~~a database including a set of reflex signatures;~~
3 a packet generator to generate and transmit a set of test packets to a remote host
4 on the network, at least part of the set of test packets including header
5 information to generate a response from the remote host that varies
6 depending upon at least one of an operating system and a service on the
7 remote host;
8 a database including a set of reflex signatures corresponding to a plurality of
9 operating systems and a plurality of services; and
10 a comparison unit to receive a set of reflex packets from the remote host
11 responsive to the test packets, and in communication with the database to
12 compare inferential information contained in the set of reflex packets to
13 the set of reflex signatures in order to identify at least one of the operating
14 system and the service and associated vulnerabilities, in communication
15 with the packet generator and the database;

16 wherein the packet generator is designed to generate and transmit a plurality of
17 test packets to the network;
18 wherein the comparison unit is designed to receive responsive packets from the
19 network and to compare inferential information from the reflex signatures;
20 and
21 wherein the comparison unit is further designed to identify a vulnerability in the
22 network based on its comparison of packet information with reflex
23 signatures.

1 37. (Currently amended) The system of claim 36, wherein the comparison
2 unit is further designed to identify an operating system type, version, and patch level and
3 a service type, version, and patch level of the remote host, ~~a host on the network~~.

1 38. (Currently amended) The system of claim 36, wherein the comparison
2 unit is designed to provide feedback information to the packet generator, and wherein the
3 packet generator is designed to use the feedback information to selectively generate test
4 packets within the set of test packets.

1 39. (Currently amended) A computer readable medium, having instructions
2 stored therein, which, when executed by a computer, causes the computer to perform the
3 steps of:
4 identifying an operating system of a remote host based on communications with
5 the remote host through the network, including identifying a version of the
6 operating system;
7 identifying a service on the port and a service of the remote host based on
8 communications with the remote host through the network, including
9 identifying a version of the service; and
10 identifying a vulnerability of the network based on information obtained from the
11 identified operating system and the identified service steps of identifying
12 an operating system and identifying a service.

1 40. (Currently amended) The computer readable medium of claim 39,
2 wherein:
3 ~~the instructions for identifying an operating system further includes instructions~~
4 ~~for identifying a patch level of the operating system; and~~
5 ~~the instructions for identifying a service further includes instructions for~~
6 identifying a patch level of the service.

1 41. (Currently amended) The computer readable medium of claim 39,
2 wherein:
3 ~~the step of identifying an operating system includes sending a first set of packets~~
4 ~~to the remote host and receiving a second set of packets from the remote~~
5 ~~host in response to the said first set of packets, and analyzing the second~~
6 ~~set of packets for inferential information indicative of the operating~~
7 ~~system; and~~
8 ~~the step of identifying a service includes sending a third set of packets to the~~
9 ~~remote host and receiving a fourth set of packets from the remote host in~~
10 ~~response to the said third set of packets, wherein information contained in~~
11 ~~the said third set of packets is based on information received in the said~~
12 ~~second set of packets, and analyzing the fourth set of packets for~~
13 ~~inferential information indicative of the service.~~; and
14 ~~the step of identifying a vulnerability includes comparing information contained~~
15 ~~in the second sequence of packets and the fourth sequence of packets to~~
16 ~~information in a database.~~

1 42. (Canceled)

1 43. (Currently amended) A method for use by a host on a network,
2 comprising:
3 receiving a first set of test packets from a remote equipment;
4 automatically sending a first set of reflexive packets to the said remote equipment
5 responsive to the first set of packets, the first set of reflexive packets

6 containing header information generated ~~according to a Request For~~
7 ~~Comment (RFC) protocol~~ and indicative of an operating system on the
8 host, including a version and patch level;
9 receiving a second set of test packets from the first test packet from remote
10 equipment; and
11 ~~automatically~~ sending a second set of reflexive packets to the said remote
12 equipment responsive to the second set of test packets, the second set of
13 reflexive packets containing header information generated ~~according to a~~
14 ~~Request For Comment (RFC) protocol~~ and indicative of a service on the
15 host, including a version and patch level;
16 ~~wherein the first set of reflexive packets includes information that enables the~~
17 ~~remote equipment to identify the operating system on the host, including a~~
18 ~~version and a patch level;~~
19 ~~wherein the second set of reflexive packets includes information that enables the~~
20 ~~remote equipment to identify the service on the host, including a version~~
21 ~~and a patch level.~~

1 44. (Currently amended) A method of examining a network, including:
2 identifying an operating system of a remote host, including a version and a patch
3 level of the operating system with a first set of packets, the first set of
4 packets comprising an operating system packet to determine the operating
5 system, an operating system version packet to determine the operating
6 system version based on the determined operating system, and an
7 operating system patch level packet to determine the operating system
8 patch level based on the determined operating system version;
9 identifying a service of the remote host, including a version and a patch level of
10 the service with a second set of packets based on the identified operating
11 system ~~at least one of the first set of packets~~, the first set of packets
12 comprising a service packet to determine the service, a service version
13 packet to determine the service version based on the determined service,

14 and a service patch level packet to determine the service patch level based
15 on the determined service version; and
16 identifying a vulnerability of the network based on information obtained from the
17 steps of identifying an operating system and identifying a service.

1 45. (Currently amended) A method of examining a network, including:
2 identifying an operating system of a remote host, including a version and a patch
3 level of the operating system, with responses to ~~nonconforming data~~
4 packets having nonconforming headers;
5 identifying a service of the remote host, including a version and a patch level of
6 the service, with responses to the nonconforming data packets; and
7 identifying a vulnerability of the network based on the identified operating system
8 and the identified service. ~~information obtained from the steps of~~
9 ~~identifying an operating system and identifying a service.~~

1 46. (New) The method of claim 1, wherein identifying a service comprises
2 directing the communications to ports of the remote host based on the identified
3 operating system.

1 47. (New) The method of claim 2, wherein the inferential information
2 comprises header information associated with the second set of packets, at least part of
3 the header information being unique to the identified operating system.

1 48. (New) The method of claim 2, wherein the inferential information
2 comprises header information associated with the fourth set of packets, at least part of the
3 header information being unique to the identified service.

1 49. (New) The method of claim 4, wherein identifying a service further
2 includes identifying a patch level of the service.